CONNECTIONS

SUMMIT

Cyber Threat Reality Check Threat to Municipalities

Wednesday February 19, 2020
Doug Westlund
Senior Vice President, Principal Consultant
AESI-US, Inc.

ELECTRICITIES
of NORTH CAROLINA, INC.

Discussion Topics

- **Introductory Remarks**
- **The Threat Landscape**
- **The Municipal Attack Surface**
- **The Ransomware Epidemic in the Municipal Sector**
- **Effective Defense Strategies**
- **Q & A**

About AESI

- Supporting utility clients since 1984 – providing engineering and management consulting services to over 500 utilities in North America and internationally
- Substantiated and proven long term public power experience with JAAs and distribution utilities
- Selected by Hometown Connections for cyber security, IT/OT and regulatory services for public power

Hometown Connections | Partner

Regulatory Compliance

sustainable compliance assurance

Cyber Security

holistic approach to risk management

Operational Technology

managing operational complexities

Energy Advisory

pragmatic engineering support

Objectives For This Session

Describe the new epidemic of ransomware attacks on municipal entities and the role that the public power utility has in the overall defensive strategy.

The Threat Landscape

"At least 174 municipal institutions suffered ransomware attacks in 2019, according to research from antivirus software provider Kaspersky. This represents a 60 percent year-over-year increase."

https://www.msspalert.com/cybersecurity-research/municipality-ransomware-attacks-2019/

The Threat Landscape

“Municipalities become new focus of ransomware attacks.”

“This broad circulation of ransomware programs has enabled the surge in attacks on municipal governments. When cyberattacks became more common a few years ago, hackers tended to target hospital servers, assuming that the institutions would pay the ransom to quickly regain access to private, time-sensitive medical records. Hospitals were quick to bolster their security systems, so hackers turned to municipalities with out-of-date hardware and servers that likely hadn’t been backed up.”

https://www.fraud-magazine.com/article.aspx?id=4295007359

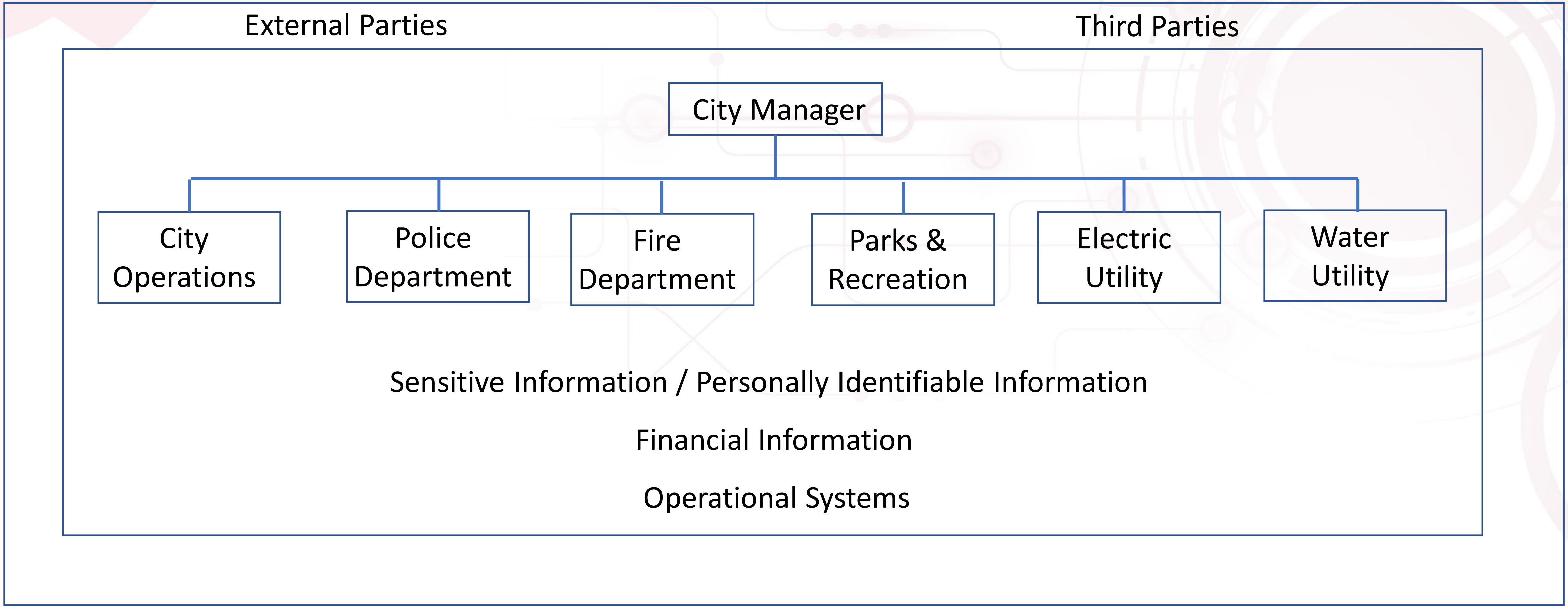
The Threat Landscape

“Hackers used to attack the average person with ransomware but have discovered that governments are much more willing to pay up because they hold more sensitive data and inherently have deeper pockets.”

“If you feed the seagulls, what's going to happen? Not only will the hackers we know about continue, but there will also be others that are attracted to ransomware if it continues to be a source of income."

https://www.cnet.com/news/ransomware-devastated-cities-in-2019-officials-hope-to-stop-a-repeat-in-2020/

The Municipal Attack Surface



External Parties

Third Parties

City Manager

City Operations

Police Department

Fire Department

Parks & Recreation

Electric Utility

Water Utility

Sensitive Information / Personally Identifiable Information

Financial Information

Operational Systems

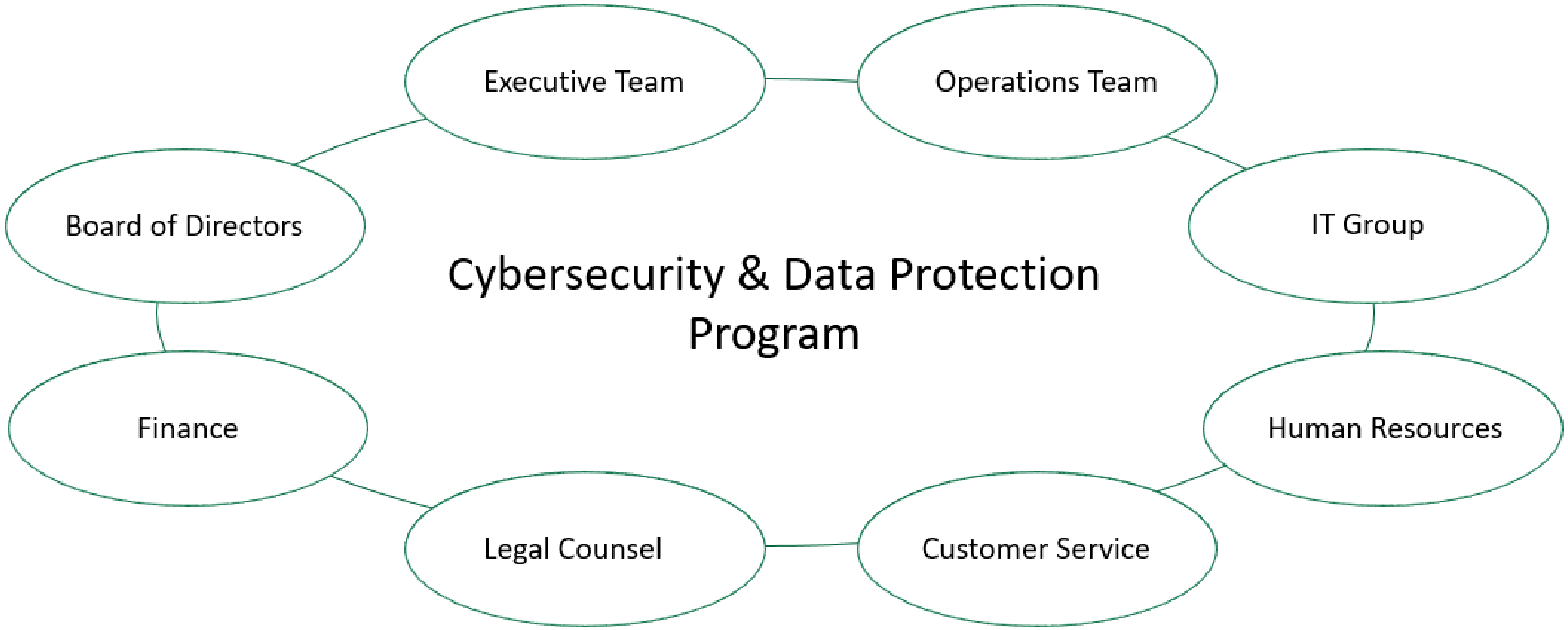
The Ransomware Epidemic in the Municipal Segment

Municipality	Ransomware Amount
Lansing Board of Water & Light, MI (2016)	$ 25 K
Lake City, FL	$ 400 K
Riviera Beach, FL	$ 600 K
Jackson County, GA	$ 400 K
Pensacola, FL	Not disclosed
Augusta, ME	$ 100 K
Albany, NY	Not disclosed
22 Cities in TX	$ 2.5 M
East Greenwich, RI	Successfully recovered

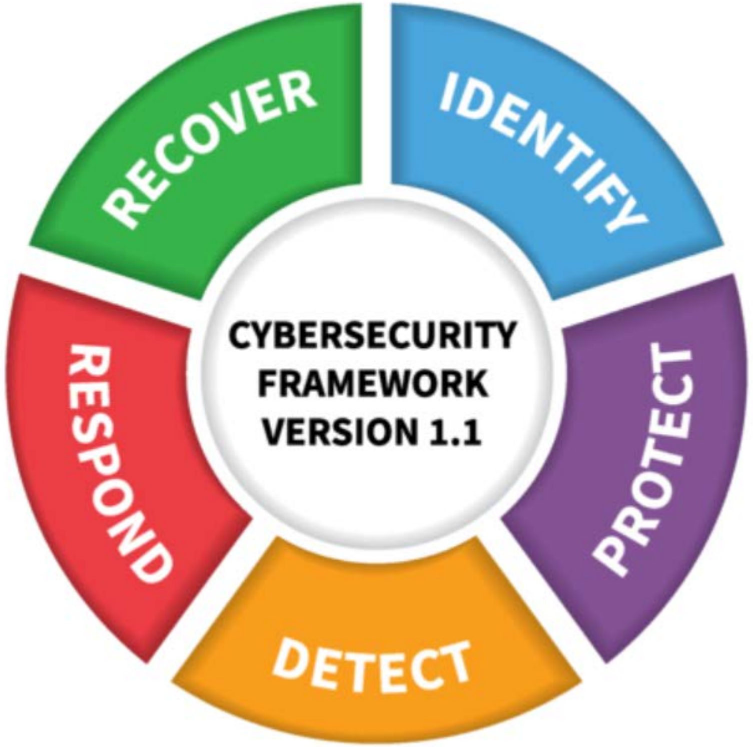
The Bottom Line for Municipalities

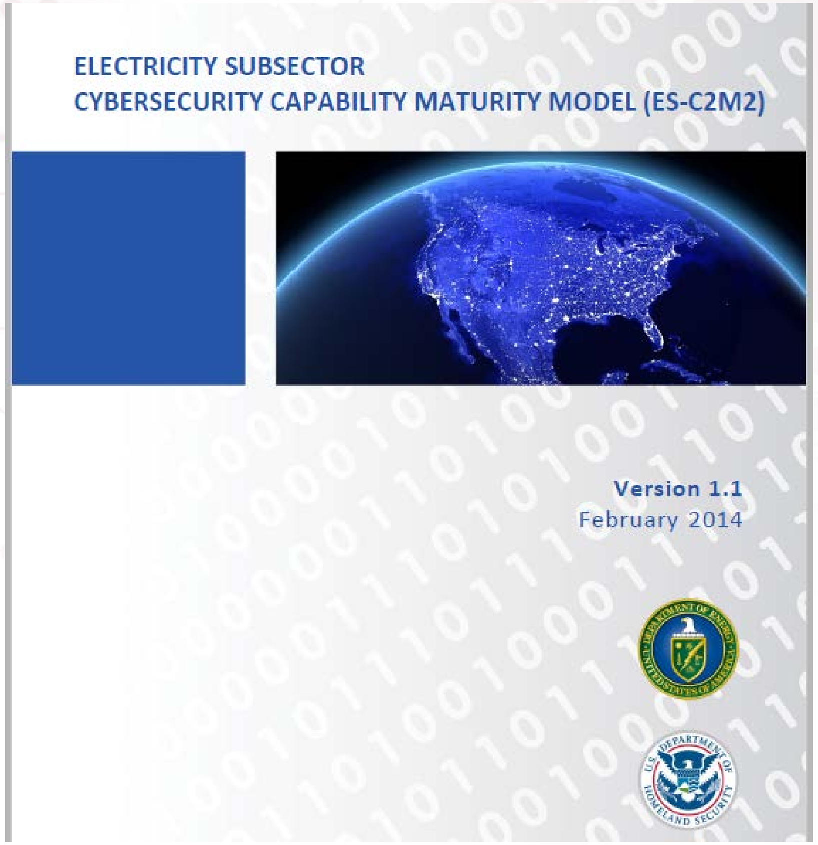
Large Attack Surface + Large Number Of Vulnerabilities + Ability To Pay = Sweet Spot For Hackers

Effective Defensive Strategies – Build a Cross-Functional Team



Effective Defensive Strategies – Align to Standards

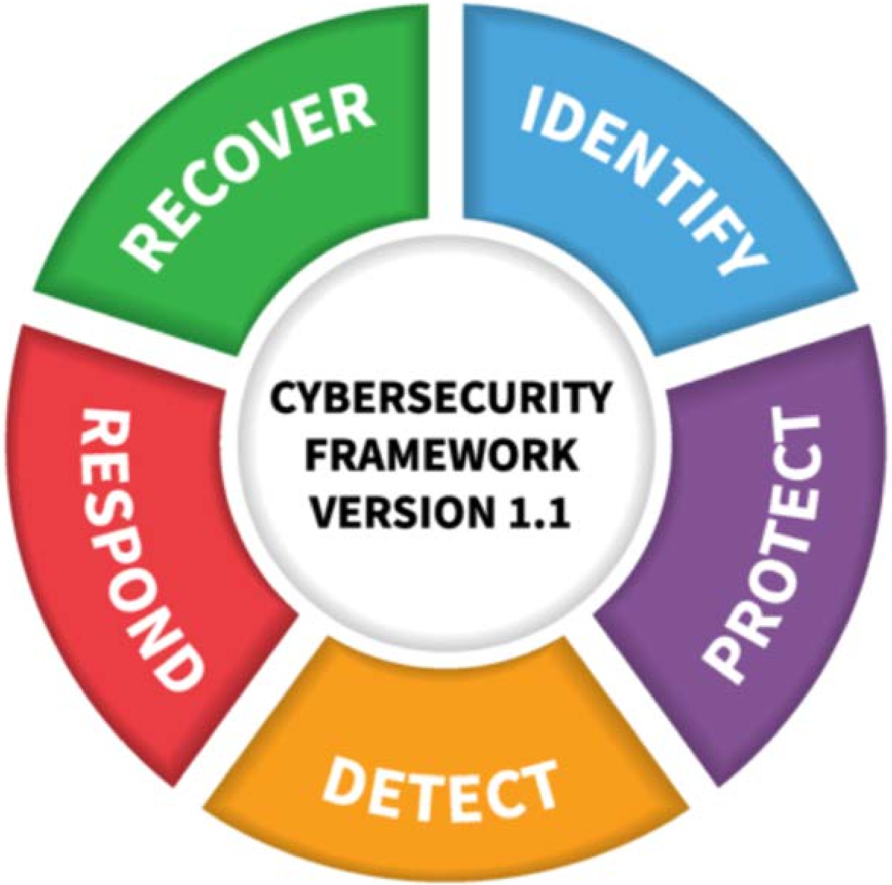




ELECTRICITY SUBSECTOR
CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)

Version 1.1
February 2014

The NIST Cybersecurity Framework (NIST CSF)

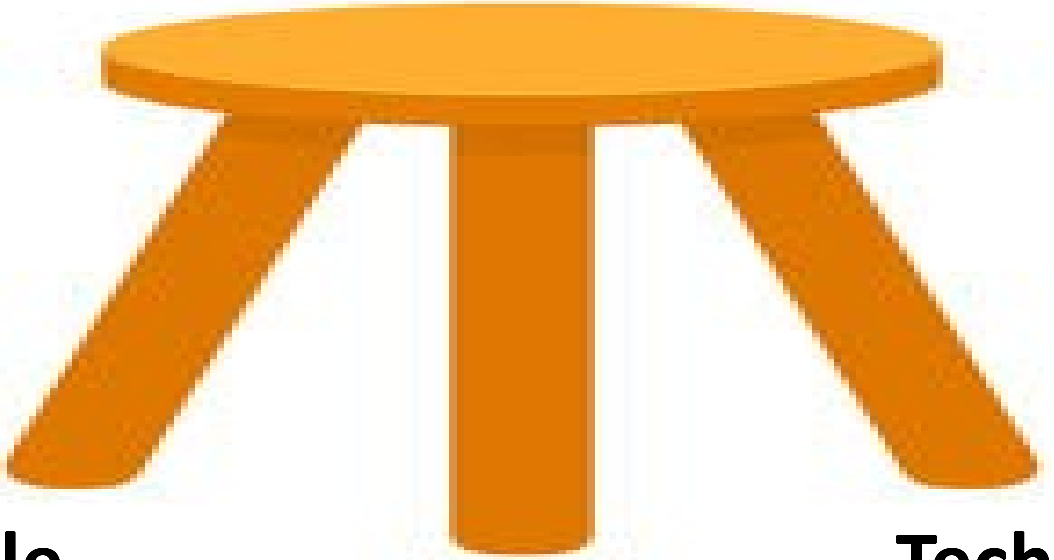


- The Industry Standard for Critical Infrastructure
- Best practices, standards-based Enterprise Framework
- Will evolve into the future
- Extensive support and guidance materials available
- Endorsed by the APPA and major industry groups
- AESI has augmented the NIST CSF to include:
  - Privacy standards
  - DOE ES-C2M2 maturity levels
  - Water controls
  - Status fields
  - “Plain English” descriptions of each control
- Security Controls:
  - 23 Control Categories (e.g. Asset Management)
  - 119 Security Controls in total including privacy

Effective Defensive Strategies – Sensitive Information

- Assign responsibilities for a Privacy Program Manager
- Determine all sources and storage of sensitive information / Personally Identifiable Information
- Delete all unnecessary information
- Vigilantly protect this information using the controls in the NIST CSF
- Develop and regularly test back up procedures

Effective Defensive Strategies – Address all Three Legs of the “Cyber Stool”



People

Process

Technology

Role of the Public Power Utility

- Can be “quarterback” for the municipality’s cyber program
  - Many AESI clients implement the program for the utilities and then expand to the municipalities
- Defending sensitive information and critical operations
- Access to industry information and support:
  - MS-ISAC threat advisory services
  - APPA resources https://www.publicpower.org/issue/cybersecurity
  - APPA Scorecard
  - Industry Conferences

Q & A

Thank You !

Doug Westlund

Senior VP, Principal Consultant

AESI Inc.

dougw@aesi-inc.com

416.997.8833

ELECTRICITIES
of NORTH CAROLINA, INC.

The energy behind public power

www.electricities.com

FOLLOW US ON SOCIAL MEDIA:

@ElectriCitiesNC

@ElectriCitiesNC

@ElectriCitiesNC

/company/ElectriCitiesNC